

Guia Completo sobre

SEGURANÇA DA INFORMAÇÃO

LGPD, LAI e Inovação no Serviço Público



Bem-vindo ao Curso de Capacitação Digital

Segurança, Privacidade e Transparência no Serviço Público

Um curso completo para servidores públicos aprenderem a proteger dados, respeitar a privacidade dos cidadãos e garantir transparência no trabalho diário

Por Que Este Curso É Importante?



No serviço público de saúde, você trabalha com informações muito sensíveis. Dados de pacientes, diagnósticos, históricos médicos — tudo isso é valioso e precisa ser protegido.

Você Aprenderá:

Resultado Esperado:

Você será capaz de aplicar medidas básicas de segurança, identificar riscos comuns, seguir procedimentos institucionais e trabalhar com confiança no ambiente digital.

SEGURANÇA DA INFORMAÇÃO

Como proteger dados institucionais e pessoais contra ameaças digitais

LGPD NA PRÁTICA

Como tratar dados de cidadãos com ética, segurança e conformidade legal

LAI E TRANSPARÊNCIA

Como garantir o direito à informação e comunicar com clareza

NOVAS TECNOLOGIAS

Como usar ferramentas digitais para melhorar produtividade e atendimento

Estrutura do Curso

Este curso é dividido em 4 módulos práticos e interativos. Cada módulo tem duração aproximada de 6 horas e inclui conteúdo, exemplos reais e exercícios.

01

MÓDULO 1: SEGURANÇA DA INFORMAÇÃO NO DIA A DIA (6h)

Proteção prática dos dados institucionais e pessoais

- Introdução à segurança digital
- Práticas essenciais de proteção
- Procedimentos institucionais
- Situações de emergência

03

MÓDULO 3: LAI E TRANSPARÊNCIA ATIVA (6h)

Acesso à informação e comunicação clara com o cidadão

- Direito à informação
- Atendimento a pedidos de informação
- Transparência na prática
- Integração LGPD-LAI

02

MÓDULO 2: LGPD NA PRÁTICA - PROTEÇÃO DE DADOS PESSOAIS (6h)

Tratamento ético e legal de informações de cidadãos

- LGPD descomplicada
- Coleta e uso de dados no atendimento
- Compartilhamento seguro
- Cenários práticos

04

MÓDULO 4: NOVAS TECNOLOGIAS E EFICIÊNCIA (6h)

Ferramentas digitais para melhorar produtividade e atendimento

- Transformação digital acessível
- Ferramentas de produtividade
- Inteligência artificial no cotidiano
- Atendimento digital ao cidadão

Total: 24 horas de capacitação. Você pode fazer no seu ritmo. Cada módulo é independente, mas recomendamos seguir a ordem.

Como Usar Este Curso

Dicas para aproveitar ao máximo sua experiência de aprendizado



Dedique Tempo

Reserve 1-2 horas por semana para estudar



Faça Anotações

Anote pontos importantes e dúvidas



Pratique

Aplique o aprendizado no seu trabalho diário



Tire Dúvidas

Consulte a supervisão quando não tiver certeza



Complete

Faça os questionários e exercícios de cada módulo

- Este curso é obrigatório para todos os servidores públicos de saúde. Ao final, você receberá um certificado de conclusão.

Dicas adicionais para otimizar seu aprendizado:

- Você pode pausar e retomar quando quiser
- Todos os slides estão disponíveis para consulta posterior
- Compartilhe conhecimento com seus colegas
- Reporte problemas ou sugestões ao seu supervisor

Vamos Começar!

Você está pronto para aprender a proteger dados, respeitar a privacidade e garantir transparência no serviço público?

Lembre-se:

- Segurança é responsabilidade de TODOS
- Você é a primeira linha de defesa
- Proteger dados é proteger pessoas
- Transparência constrói confiança
- Tecnologia é uma ferramenta, não uma ameaça

Próximo Passo:

Vamos começar com o MÓDULO 1: SEGURANÇA DA INFORMAÇÃO NO DIA A DIA

Neste módulo, você aprenderá:

- Por que a segurança importa
- Como criar senhas fortes
- Como identificar golpes e phishing
- Como proteger seus dispositivos
- Como guardar dados com segurança
- O que fazer em emergências

Boa sorte! 



MÓDULO 1: SEGURANÇA DA INFORMAÇÃO NO DIA A DIA

Proteção Prática dos Dados Institucionais e Pessoais

Aprenda a proteger dados, identificar riscos e seguir procedimentos de segurança no seu trabalho diário

Por Que Segurança da Informação É Tão Importante?



No serviço público de saúde, você trabalha com informações muito sensíveis. Dados de pacientes, diagnósticos, históricos médicos — tudo isso é valioso e precisa ser protegido.

Riscos Reais:

- Vazamento de dados: Informações de pacientes expostas na internet
- Fraude: Criminosos usam dados para abrir contas ou fazer compras
- Prejuízo institucional: Perda de confiança dos cidadãos
- Consequências legais: Multas e processos por não proteger dados

Histórias Reais:

Em 2023, um hospital brasileiro teve dados de 50 mil pacientes vazados por falta de segurança básica. Resultado: multa de R\$ 2 milhões e perda de confiança pública.

Sua Responsabilidade:

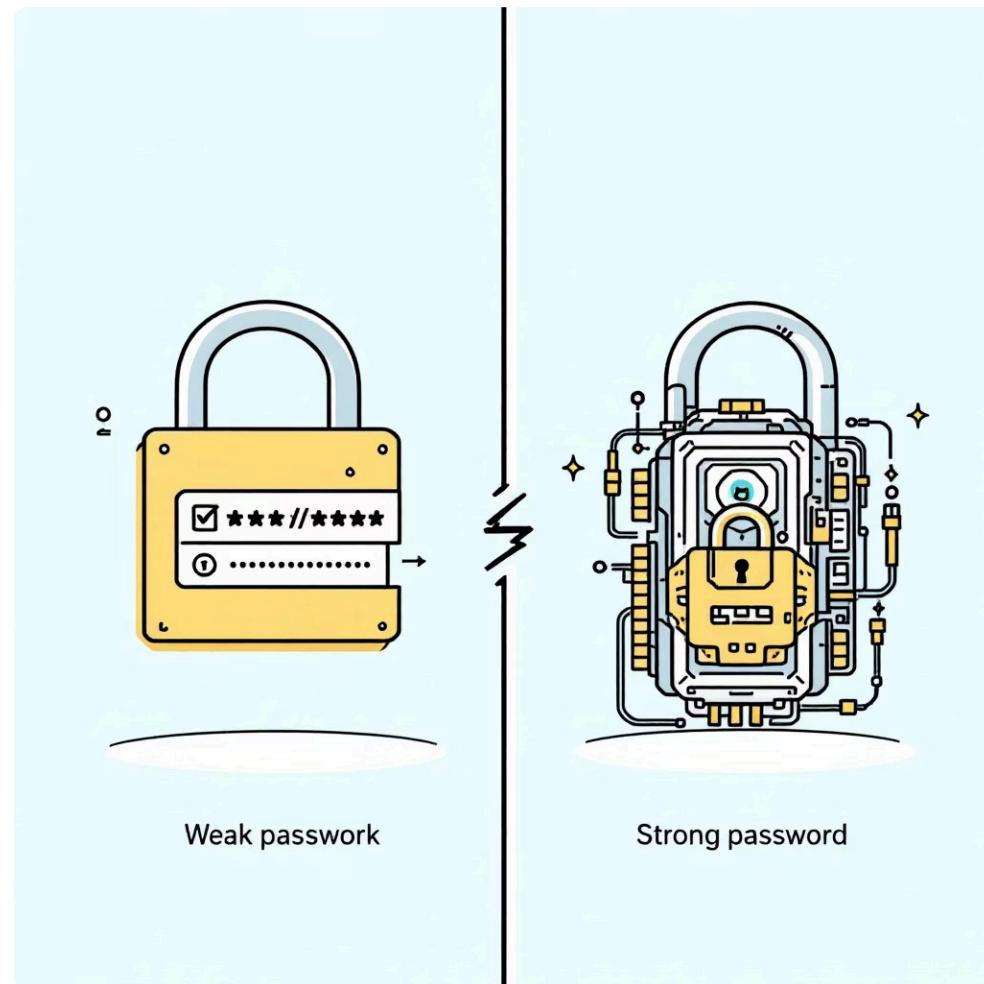
Você é a primeira linha de defesa. Senhas fracas, e-mails abertos, dispositivos desprotegidos — tudo isso pode levar a vazamentos.

Lembre-se:

Proteger dados não é apenas obrigação legal, é ética profissional.

Criando Senhas Realmente Fortes

Uma senha fraca é como deixar a porta de sua casa aberta. Criminosos conseguem entrar facilmente. Uma senha forte é como uma fechadura de segurança.



✗ SENHAS FRACAS:

- 123456
- senha123
- admin
- seu nome ou data de nascimento
- mesma senha em vários lugares

✓ SENHAS FORTES:

- Mínimo 12 caracteres
- Misture: MAIÚSCULAS, minúsculas, números, símbolos
- Exemplo: Br@sil2024#Saúde!
- Única para cada sistema
- Sem informações pessoais

- Tem pelo menos 12 caracteres?
- Tem letras maiúsculas E minúsculas?
- Tem números?
- Tem símbolos (@, #, !, \$)?
- Não contém seu nome ou data de nascimento?
- É diferente de outras senhas suas?

Use um gerenciador de senhas (como Bitwarden ou 1Password) para guardar senhas fortes com segurança.

Identificando E-mails Suspeitos e Phishing

Phishing é quando criminosos enviam e-mails falsos fingindo ser do banco, do chefe ou de empresas conhecidas para roubar suas senhas e dados. É uma das ameaças mais comuns no ambiente digital.

🚩 SINAIS DE ALERTA:

- Remetente estranho ou parecido com alguém conhecido
- Pedido urgente para clicar em link ou abrir anexo
- Erros de digitação ou português ruim
- Ameaças ('sua conta será bloqueada')
- Ofertas muito boas para ser verdade

✗ NUNCA FAÇA:

- Clique em links de e-mails suspeitos
- Abra anexos de remetentes desconhecidos
- Responda com suas senhas ou dados pessoais
- Baixe arquivos de e-mails não confiáveis

✓ SEMPRE FAÇA:

- Verifique o endereço de e-mail completo
- Passe o mouse sobre links para ver o URL real
- Quando em dúvida, ligue para a pessoa
- Reporte e-mails suspeitos ao TI

📞 SE RECEBER UM E-MAIL SUSPEITO:

- Não clique em nada
- Reporte ao setor de TI
- Delete o e-mail
- Avise seus colegas

Exemplo de phishing: E-mail que parece do seu chefe pedindo para transferir dinheiro urgentemente. Solução: Ligue para o chefe para confirmar.

Segurança em Dispositivos Móveis



Seu Celular Também Precisa de Proteção

Muitos servidores acessam sistemas de saúde pelo celular ou tablet. Se o aparelho cair em mãos erradas sem proteção adequada, dados sensíveis podem ser expostos.

01

Use Senha ou Biometria:

Desbloqueie com PIN, padrão ou impressão digital

02

Atualize o Sistema:

Instale atualizações de segurança regularmente

03

Cuidado com Apps:

Baixe apenas de lojas oficiais (Google Play, App Store)

04

Não Use Wi-Fi Público:

Evite acessar sistemas sensíveis em redes abertas

05

Ative Localização Remota:

Se perder o celular, você consegue rastreá-lo

- ▢ Celular tem senha ou biometria?
- ▢ Sistema operacional está atualizado?
- ▢ Você só baixa apps de lojas oficiais?
- ▢ Não acessa dados sensíveis em Wi-Fi público?
- ▢ Sabe como rastrear seu celular se perder?

Se perder seu celular com dados de trabalho, avise o TI imediatamente!

Onde Salvar Arquivos com Segurança

Nem todo lugar é seguro para guardar arquivos. Você precisa saber onde salvar cada tipo de informação.



Nuvem Institucional (OneDrive, Google Drive corporativo)

MELHOR OPÇÃO:
Criptografada, com backup automático, acesso controlado



Computador da Instituição

BOM: Protegido por antivírus e firewall, mas faça backup



Celular Pessoal

EVITE : Dados de trabalho não devem estar em dispositivos pessoais

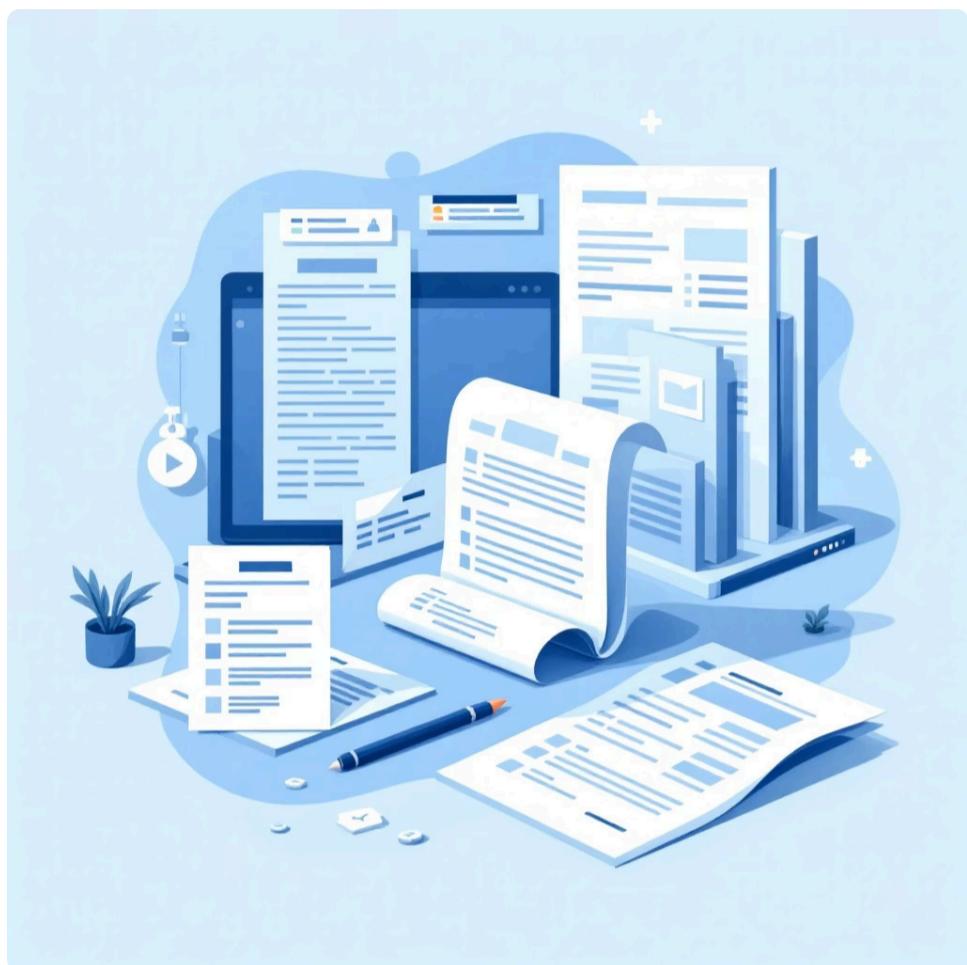


Pen Drive ou HD Externo

RISCO: Fácil de perder ou roubar. Se usar, criptografe!

Regra de Ouro: Dados de trabalho SEMPRE na nuvem institucional ou computador da instituição. Nunca em dispositivos pessoais ou pen drives desprotegidos.

Classificação de Documentos: Público, Restrito, Sigilosos



Nem todo documento é igual. A lei exige que você classifique informações corretamente para protegê-las adequadamente.

● PÚBLICO

Pode ser compartilhado com qualquer pessoa

Exemplos: Horários de funcionamento, protocolos gerais, informações sobre serviços

Proteção: Nenhuma especial

● RESTRITO

Pode ser compartilhado apenas com pessoas autorizadas

Exemplos: Dados de pacientes, informações financeiras, relatórios internos

Proteção: Acesso controlado, senha, criptografia

● SIGILOSO

Acesso muito limitado, apenas pessoas específicas

Exemplos: Investigações, informações de segurança, dados de autoridades

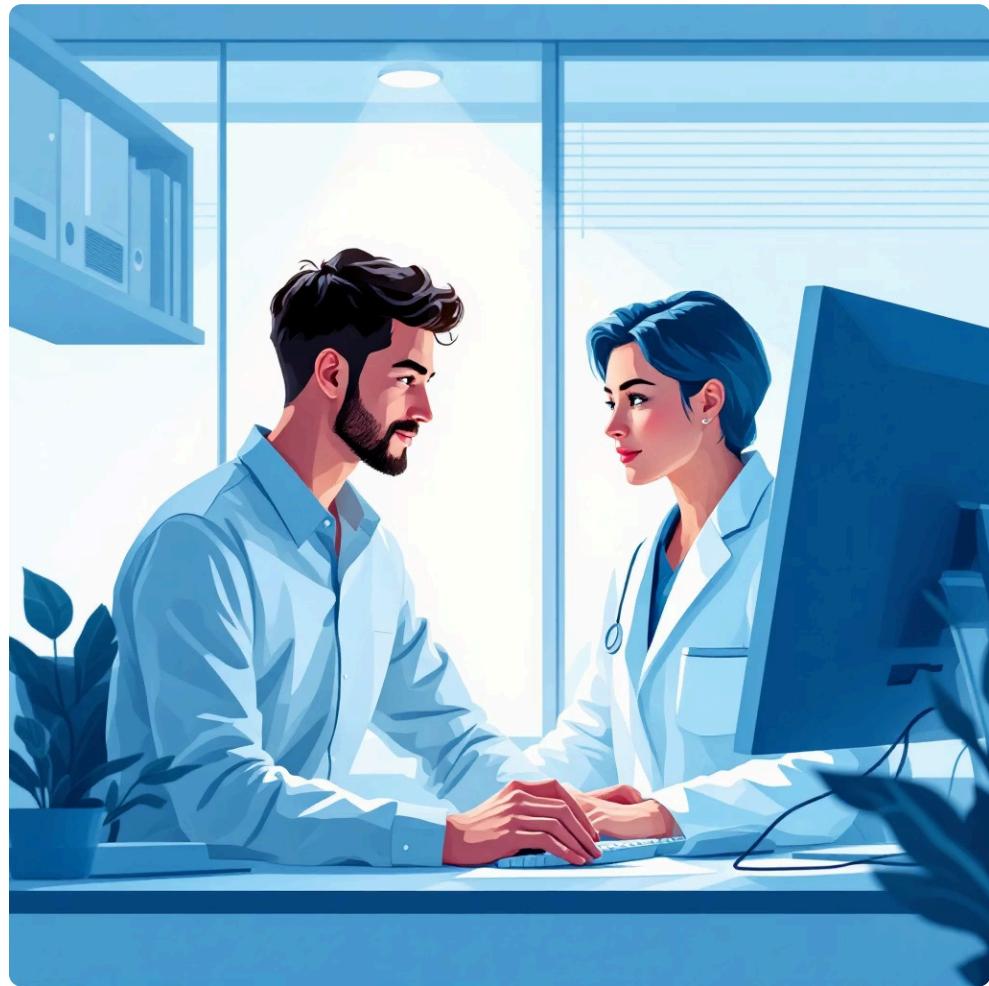
Proteção: Máxima segurança, acesso rastreado

- Você sabe classificar cada documento?
- Você guarda documentos restritos com segurança?
- Você nunca compartilha documentos sigilosos?
- Você sabe quem pode acessar cada tipo?

Dica: Quando em dúvida, classifique como RESTRITO. É melhor ser cauteloso.

Backup: Por Que e Como Fazer

Backup é uma cópia de segurança de seus arquivos. Se algo der errado (vírus, falha do computador, acidente), você não perde tudo.



Por Que Fazer Backup?

- Proteção contra vírus e ransomware
- Recuperação de arquivos deletados por acidente
- Proteção contra falhas de hardware
- Conformidade com leis de proteção de dados

Como Fazer Backup:

1. Use a nuvem institucional (automático)
2. Faça backup semanal em HD externo criptografado
3. Teste o backup: Verifique se consegue restaurar

Frequência Recomendada:

- Dados críticos: Diariamente
- Dados importantes: Semanalmente
- Dados gerais: Mensalmente

Checklist de Backup:

- Você faz backup regularmente?
- Seu backup está criptografado?
- Você testou restaurar um arquivo?
- Você guarda o backup em local seguro?

Lembre-se: Um backup que você não testou é um backup que não funciona!

Principais Aprendizados do Módulo 1



Senhas Fortes: Mínimo 12 caracteres, misture tipos



E-mail Seguro: Identifique phishing, nunca clique em links suspeitos



Dispositivos Móveis: Sempre protegidos com senha ou biometria



Armazenamento: Nuvem institucional é o melhor lugar



Classificação: Público, Restrito, Sigiloso



Emergências: Avise o TI imediatamente

Você Completou o Módulo 1!

Segurança da Informação no Dia a Dia



Parabéns! Você agora entende os princípios fundamentais de segurança da informação e como aplicá-los no seu trabalho diário.

Lembre-se dos Princípios Fundamentais:

Você é a primeira linha de defesa contra ameaças digitais. Sua vigilância protege não apenas seus dados, mas os de todos os pacientes que confiamos em nosso cuidado.

Nos vemos no próximo módulo!

SENHAS E ACESSO

- Senhas fortes com 12+ caracteres
- Nunca compartilhe suas credenciais
- Mude senha regularmente
- Use autenticação de dois fatores

E-MAIL E COMUNICAÇÃO

- Identifique phishing e golpes
- Nunca clique em links suspeitos
- Verifique o remetente
- Reporte e-mails suspeitos

DISPOSITIVOS E ARMAZENAMENTO

- Celular sempre protegido
- Nuvem institucional para dados
- Backup regular e testado
- Nunca use pen drives desprotegidos

DOCUMENTOS E DESCARTE

- Classifique corretamente
- Guarde com segurança
- Destrua fisicamente quando necessário
- Delete permanentemente arquivos digitais

EMERGÊNCIAS

- Avise o TI imediatamente
- Não tente resolver sozinho
- Documente o incidente
- Aprenda com o ocorrido

Situações de Emergência: O Que Fazer

Às vezes, algo dá errado. Você suspeita de uma invasão, seu computador está lento, recebeu um e-mail estranho. O que fazer?



SUSPEITA DE INVASÃO:

- Desligue o computador imediatamente
- Não tente 'investigar' sozinho
- Avise o setor de TI
- Mude sua senha em outro computador

COMPUTADOR LENTO OU TRAVANDO:

- Pode ser vírus ou malware
- Avise o TI para verificar
- Não instale programas para 'limpar'
- Não clique em pop-ups de 'limpeza'

RECEBEU E-MAIL SUSPEITO:

- Não clique em links
- Não abra anexos
- Reporte ao TI
- Delete o e-mail

PERDEU DADOS OU ARQUIVO FOI DELETADO:

- Avise o TI imediatamente
- Não tente recuperar sozinho
- Quanto antes avisar, melhor a chance de recuperação
- Tenha um backup atualizado

Contato de Emergência TI: [número/e-mail]. Disponível 24/7 para emergências de segurança.

MÓDULO 2: LGPD NA PRÁTICA - PROTEÇÃO DE DADOS PESSOAIS

Lei Geral de Proteção de Dados Pessoais

Aprenda a tratar dados de cidadãos com ética, segurança e conformidade legal

O Que São Dados Pessoais? Exemplos do Cotidiano

Dados pessoais são qualquer informação que identifica ou pode identificar uma pessoa. Na saúde, praticamente **TUDO** é considerado dado pessoal sensível.



Identificação Pessoal

Nome, CPF, RG, CNH, Passaporte



Dados de Saúde

Diagnóstico, histórico médico, medicamentos, alergias



Resultados Médicos

Exames, testes, análises clínicas



Informações de Contato

Telefone, endereço, e-mail, redes sociais

Dados pessoais sensíveis (saúde, origem racial, religião) têm proteção EXTRA. Você precisa de consentimento explícito para coletar e usar.

- ▢ Você sabe o que é dado pessoal?
- ▢ Você entende que dados de saúde são sensíveis?
- ▢ Você sabe quando precisa de consentimento?
- ▢ Você protege dados pessoais com segurança?

Princípios Básicos da LGPD: Finalidade, Necessidade, Transparência

A LGPD se baseia em princípios que guiam como você deve tratar dados pessoais.



🎯 FINALIDADE: Você só coleta dados para um propósito específico
Exemplo: Coleta nome e diagnóstico para atendimento, não para vender para terceiros

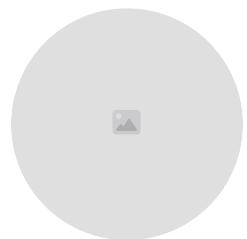
✂️ NECESSIDADE: Coleta apenas o mínimo necessário
Exemplo: Para marcar consulta, precisa de nome e telefone. Não precisa de renda ou religião

📢 TRANSPARÊNCIA: Você explica ao cidadão por que coleta dados
Exemplo: 'Preciso do seu CPF para registrar no sistema de saúde. Seus dados serão protegidos.'

Esses princípios não são sugestões. São obrigações legais. Violá-los pode resultar em multa e processo.

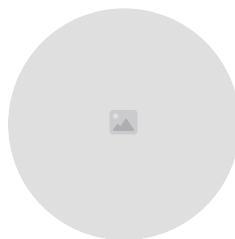
Direitos dos Cidadãos: Acesso, Correção, Exclusão

A LGPD garante direitos específicos aos cidadãos sobre seus dados. Você precisa respeitá-los.



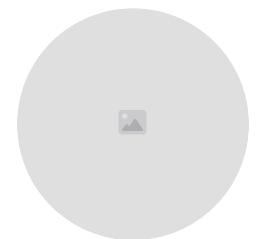
Direito de Acesso:
O cidadão pode
pedir para VER
todos os seus
dados

Você tem 15 dias para
fornecer uma cópia
completa



**Direito de
Correção:** Pode
solicitar
CORREÇÃO de
informações
incorrectas

Se o dado está errado,
você deve corrigir
imediatamente



**Direito de
Exclusão:** Pode
pedir para
DELETAR seus
dados

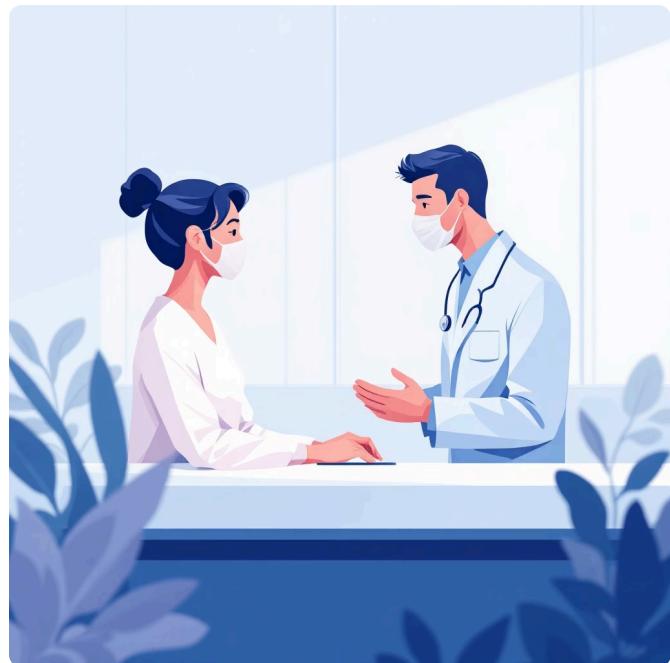
Se não há mais
necessidade legal,
você deve apagar
(com exceções)

- ☐ Se um cidadão pedir para acessar, corrigir ou deletar seus dados, você DEVE atender ou encaminhar para o responsável. Isso não é opcional.

- Você sabe como responder a pedido de acesso?
- Você sabe como corrigir dados incorretos?
- Você sabe quando pode deletar dados?
- Você tem processo para isso na instituição?

O Que Posso Perguntar ao Cidadão?

Nem toda pergunta é apropriada. Você só pode coletar dados que são necessários para o atendimento.



✓ POSSO PERGUNTAR: Nome, data de nascimento, CPF, endereço, telefone

Necessário para identificar e contatar o paciente

✓ POSSO PERGUNTAR: Histórico médico, alergias, medicamentos atuais

Necessário para atendimento seguro

✗ NÃO POSSO PERGUNTAR: Renda, religião, orientação sexual, origem racial

Não é necessário para atendimento. É discriminatório

✗ NÃO POSSO PERGUNTAR: Dados de terceiros (família, amigos)

Você só coleta dados da pessoa que está sendo atendida

Quando em dúvida, pergunte-se: 'Preciso realmente dessa informação para atender bem esse paciente?' Se a resposta é não, não pergunte.

Como Justificar a Coleta de Informações

Quando você coleta dados, o cidadão tem direito de saber por quê. Você precisa explicar claramente.



01

Seja Transparente

Explique exatamente por que você precisa daquele dado

02

Seja Claro

Use linguagem simples, não jargão técnico

03

Seja Honesto

Não invente motivos. Diga a verdade

04

Registre

Documente que você explicou e o cidadão consentiu

Exemplo 1: 'Preciso do seu CPF para registrar você no sistema de saúde. Seus dados serão protegidos e usados apenas para seu atendimento.'

Exemplo 2: 'Preciso saber se você tem alergias para prescrever medicamentos com segurança.'

Exemplo 3: 'Preciso do seu telefone para entrar em contato se precisarmos remarcar sua consulta.'

Importante: Coleta sem justificativa é violação da LGPD. Sempre explique ao cidadão.

Consentimento: Quando É Necessário e Como Registrar

Consentimento é quando o cidadão autoriza você a coletar e usar seus dados. Nem sempre é necessário, mas quando é, deve ser registrado.



✓ CONSENTIMENTO NECESSÁRIO: Coleta de dados sensíveis (saúde, origem racial, religião)

Como: Formulário assinado ou registro digital

✓ CONSENTIMENTO NECESSÁRIO: Compartilhamento com terceiros

Como: Autorização específica por escrito

✗ CONSENTIMENTO NÃO NECESSÁRIO: Dados necessários para atendimento

Por quê: Você tem obrigação legal de coletar (CPF, nome, diagnóstico)

✗ CONSENTIMENTO NÃO NECESSÁRIO: Dados já coletados para outro propósito

Por quê: Já foi autorizado anteriormente

- ▢ Você sabe quando precisa de consentimento?
- ▢ Você tem formulário de consentimento?
- ▢ Você guarda o consentimento no prontuário?
- ▢ Você explica o que está consentindo?

Importante: Consentimento deve ser LIVRE, INFORMADO e ESPECÍFICO. Não pode ser forçado ou genérico.

Menor de Idade e Dados Sensíveis: Cuidados Especiais

Crianças e adolescentes têm proteção EXTRA na LGPD. Você precisa de cuidados especiais ao coletar dados deles.

01

Menor de 13 anos: Você PRECISA de consentimento dos pais/responsáveis

02

13 a 18 anos: Você pode coletar com consentimento do adolescente, mas é bom avisar os pais

03

Dados Sensíveis: Sempre precisa de consentimento, independente da idade

04

Explique Claramente: Use linguagem que a criança/adolescente entenda

05

Registre Tudo: Guarde o consentimento dos pais/responsáveis

Exemplo 1: Criança de 10 anos com suspeita de abuso. Você coleta dados com consentimento dos pais.

Exemplo 2: Adolescente de 16 anos com depressão. Você coleta dados com consentimento dele, mas avisa os pais.

Exemplo 3: Criança com alergia. Você coleta informação de alergia com consentimento dos pais.

Importante: Dados de menores são MUITO sensíveis. Qualquer violação pode resultar em processo criminal.

Quando e Como Compartilhar Dados Entre Setores

Às vezes, você precisa compartilhar dados de um paciente com outro setor. Isso é permitido, mas com regras.

COMPARTILHE: Com profissionais envolvidos no atendimento do paciente

How: Use canais seguros (e-mail criptografado, sistema interno)

COMPARTILHE: Com supervisores para qualidade do serviço

How: Apenas dados necessários, com justificativa

NÃO COMPARTILHE: Com colegas que não estão envolvidos no caso

Why: Violação do princípio de necessidade

NÃO COMPARTILHE: Em conversas informais, grupos de WhatsApp, redes sociais

Why: Violação grave da LGPD

Checklist:

- Você sabe quem pode acessar dados do paciente?
- Você usa canais seguros para compartilhar?
- Você compartilha apenas o necessário?
- Você documenta quem acessou os dados?

 **Importante:** Compartilhamento sem necessidade é crime. Você pode ser responsabilizado pessoalmente.

Canais Seguros para Envio de Informações

Quando você precisa enviar dados de pacientes, o canal que usa importa muito. Alguns são seguros, outros são perigosos.



✓ SEGURO: E-mail criptografado da instituição

Protegido por senha e criptografia

✓ SEGURO: Sistema interno da instituição

Acesso controlado, rastreado, auditado

✗ INSEGURO: E-mail pessoal (Gmail, Hotmail)

Não é criptografado, pode ser hackeado

✗ INSEGURO: WhatsApp, SMS, redes sociais

Não é seguro, deixa rastro, pode ser interceptado

Checklist:

- Você sabe qual é o canal seguro da sua instituição?
- Você nunca usa e-mail pessoal para dados de trabalho?
- Você nunca compartilha em WhatsApp ou redes sociais?
- Você criptografa dados sensíveis?

Importante: Enviar dados sensíveis por canal inseguro é violação grave. Sempre use canais aprovados pela instituição.

Anonimização: Como Proteger Dados em Relatórios

Às vezes, você precisa compartilhar dados em relatórios ou planilhas. Você pode fazer isso com segurança removendo informações que identificam pessoas.



01

Identifique

Quais dados identificam a pessoa?
(nome, CPF, data de nascimento)

02

Remova

Delete ou substitua essas informações

03

Mantenha

Informações estatísticas (número de pacientes, diagnósticos, idades)

04

Verifique

Certifique-se de que ninguém consegue identificar a pessoa

Exemplo 1 - ANTES: 'João Silva, CPF 123.456.789-00, 45 anos, hipertensão'

DEPOIS: 'Paciente 001, 45 anos, hipertensão'

Exemplo 2 - ANTES: 'Maria Santos, diabética, renda R\$ 2.000'

DEPOIS: 'Paciente 002, diabético, renda baixa'

Exemplo 3 - ANTES: 'Tabela com nomes e diagnósticos'

DEPOIS: 'Tabela com número de pacientes por diagnóstico'

Importante: Anonimização bem feita permite compartilhar dados sem violar privacidade. Sempre anonimize quando possível.

Cenários Práticos: Estude de Casos Reais

Identifique Práticas Corretas e Incorretas

Para cada cenário, identifique: Isso está correto ou viola a LGPD?

CENÁRIO: Você recebe um pedido de um pesquisador para acessar prontuários de 100 pacientes para um estudo.

- INCORRETO: Compartilhar prontuários completos com nomes
- CORRETO: Compartilhar dados anonimizados com consentimento dos pacientes

CENÁRIO: Seu chefe pede para você enviar uma lista de pacientes com diabetes por WhatsApp.

- INCORRETO: Enviar lista com nomes e diagnósticos por WhatsApp
- CORRETO: Usar e-mail criptografado ou sistema interno, anonimizar se possível

CENÁRIO: Um familiar liga pedindo informações sobre o paciente.

- INCORRETO: Compartilhar diagnóstico ou histórico sem autorização
- CORRETO: Pedir autorização por escrito do paciente antes de compartilhar

CENÁRIO: Você precisa fazer um relatório mensal de atendimentos.

- INCORRETO: Listar nomes e diagnósticos de todos os pacientes
- CORRETO: Usar estatísticas (número de pacientes, diagnósticos mais comuns)

CENÁRIO: Um paciente pede para ver todos os seus dados.

- INCORRETO: Negar o pedido ou demorar meses
- CORRETO: Fornecer cópia completa em até 15 dias

Checklist para decisões diárias:

- Preciso realmente dessa informação?
- Tenho consentimento do paciente?
- Estou usando canal seguro?
- Estou compartilhando apenas o necessário?
- Posso anonimizar?
- Estou documentando tudo?

Importante: Quando em dúvida, consulte a supervisão. Melhor ser cauteloso do que violar a LGPD.

MÓDULO 3: LAI E TRANSPARÊNCIA ATIVA

Lei de Acesso à Informação - Transparência Ativa e Passiva

Aprenda a garantir o direito à informação e comunicar com clareza com os cidadãos

Transparência Ativa vs. Passiva

Existem duas formas de transparência. Você precisa entender a diferença para cumprir a lei corretamente.



Transparência ATIVA: Você publica informações SEM ser pedido

Você coloca dados no portal, site, relatórios públicos. O cidadão não precisa pedir nada. Exemplos: orçamento, licitações, salários de servidores, protocolos de atendimento

Transparência PASSIVA: Você responde quando o cidadão PEDE

Cidadão faz um pedido formal (LAI) e você tem 20 dias para responder. Exemplos: 'Quantos pacientes foram atendidos em janeiro?', 'Qual é o protocolo de diabetes?'

Ambas são obrigatórias por lei. Transparência ativa é mais eficiente porque reduz pedidos.

Diferença: Informação Pública vs. Sigilosa

Nem toda informação pode ser compartilhada. A lei define claramente o que é público e o que é sigiloso.



INFORMAÇÃO PÚBLICA

Orçamento, licitações, salários de servidores, protocolos

INFORMAÇÃO PÚBLICA

Estatísticas gerais (número de atendimentos, doenças mais comuns)

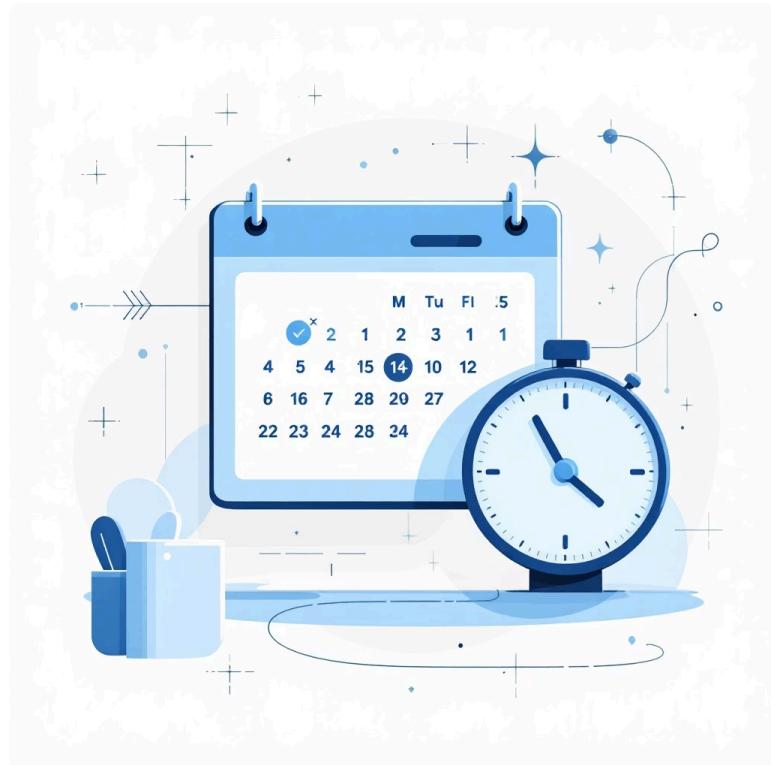
INFORMAÇÃO SIGILOSA

Dados pessoais de pacientes (nome, CPF, diagnóstico)

INFORMAÇÃO SIGILOSA

Informações que prejudiquem a segurança pública ou investigações

- ☐ Quando em dúvida, consulte a supervisão. Publicar informação sigilosa é crime.



Prazos Legais e Consequências

A LAI estabelece prazos claros. Não cumprir tem consequências.

01

Pedido recebido → Emita protocolo no mesmo dia

02

Você tem 20 DIAS para responder (contados a partir do protocolo)

03

Se precisar de mais tempo → Peça extensão de 10 dias (uma única vez)

04

Responda com clareza, completude e em linguagem acessível

05

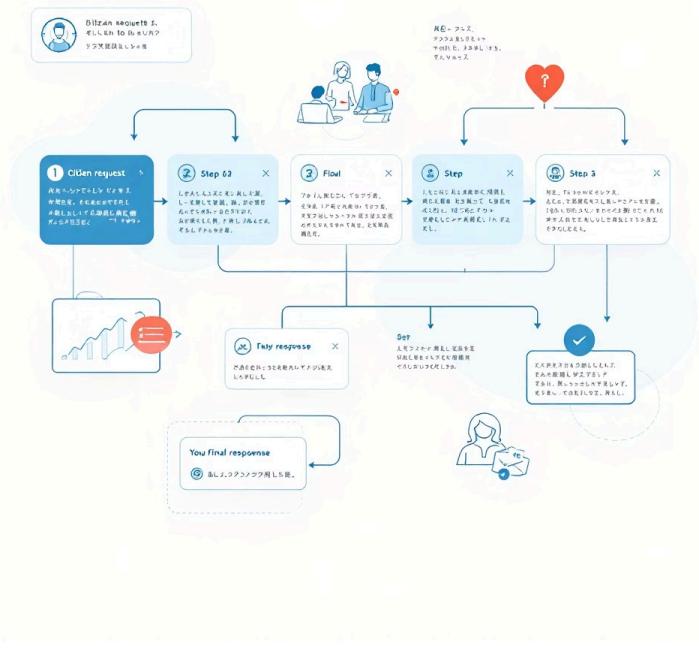
Se negar → Justifique com base em lei específica

❑ Consequências do descumprimento:

- Advertência e multa para o servidor
- Processo administrativo
- Possível ação judicial
- Dano à reputação da instituição

Cumprir prazos é obrigação legal, não sugestão.

Fluxo de Atendimento a Pedidos de Informação



Entenda o caminho que um pedido de LAI percorre desde a chegada até a resposta.

01

Cidadão faz pedido (por escrito, e-mail, formulário online ou presencialmente)

02

Servidor recebe e REGISTRA o pedido no sistema

03

Emite PROTOCOLO com número único e data

04

Encaminha para o setor responsável pela informação

05

Setor prepara resposta clara e completa em até 20 dias

06

Resposta é enviada ao cidadão (por e-mail, presencialmente ou conforme solicitado)

Importante: Cada etapa deve ser documentada. Isso garante rastreabilidade e conformidade legal.

Como Formular Respostas Claras e Completas

Uma boa resposta a um pedido de LAI é clara, completa e acessível. Não é apenas fornecer dados brutos.



Comece com um resumo: Responda a pergunta principal em 2-3 linhas

Seja específico: Forneça exatamente o que foi pedido, nada mais, nada menos

Use linguagem clara: Evite jargão técnico. Explique termos complexos

Organize bem: Use títulos, listas, tabelas para facilitar a leitura

Cite fontes: Indique onde os dados vieram (sistema, relatório, etc.)

Exemplo:

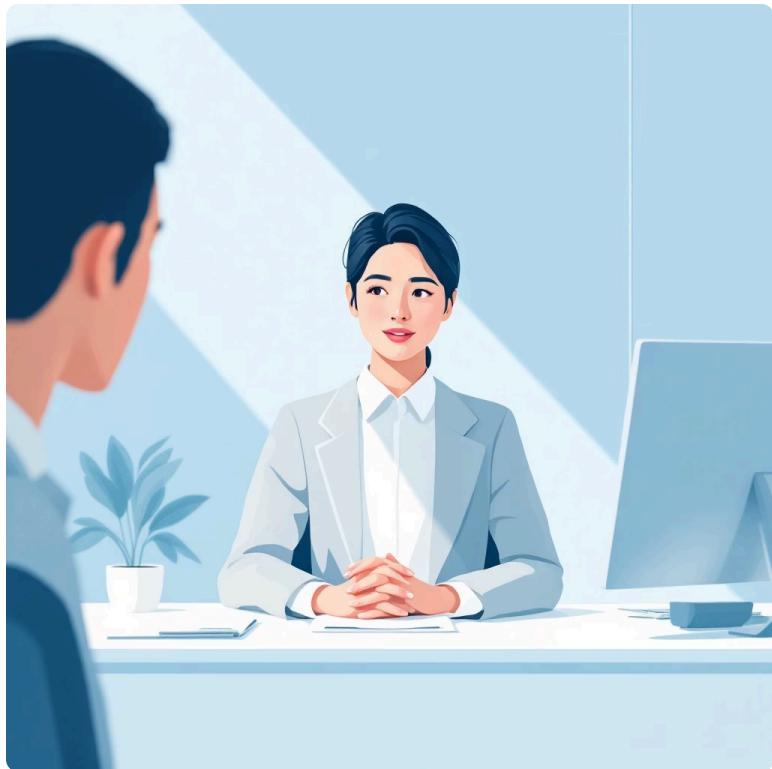
Pergunta: 'Quantos pacientes com hipertensão foram atendidos em janeiro?'

Resposta ruim: 'Conforme dados do SISREG, 347 pacientes'

Resposta boa: 'Em janeiro de 2026, foram atendidos 347 pacientes com diagnóstico de pressão alta (hipertensão). Esses dados foram extraídos do sistema de registros de saúde (SISREG) em 3 de fevereiro de 2026.'

Negativa Justificada: Quando e Como Dizer 'Não'

Às vezes, você precisa negar um pedido de LAI. Isso é permitido, mas DEVE ser justificado com base em lei.



01

Identifique o motivo legal:

Informação sigilosa? Dados pessoais? Segurança pública?

02

Cite a lei específica:

'Conforme artigo X da Lei Y, essa informação é sigilosa porque...'

03

Explique claramente:

O cidadão tem direito de entender por que foi negado

04

Indique recurso:

'Você pode recorrer desta decisão ao [órgão responsável]'

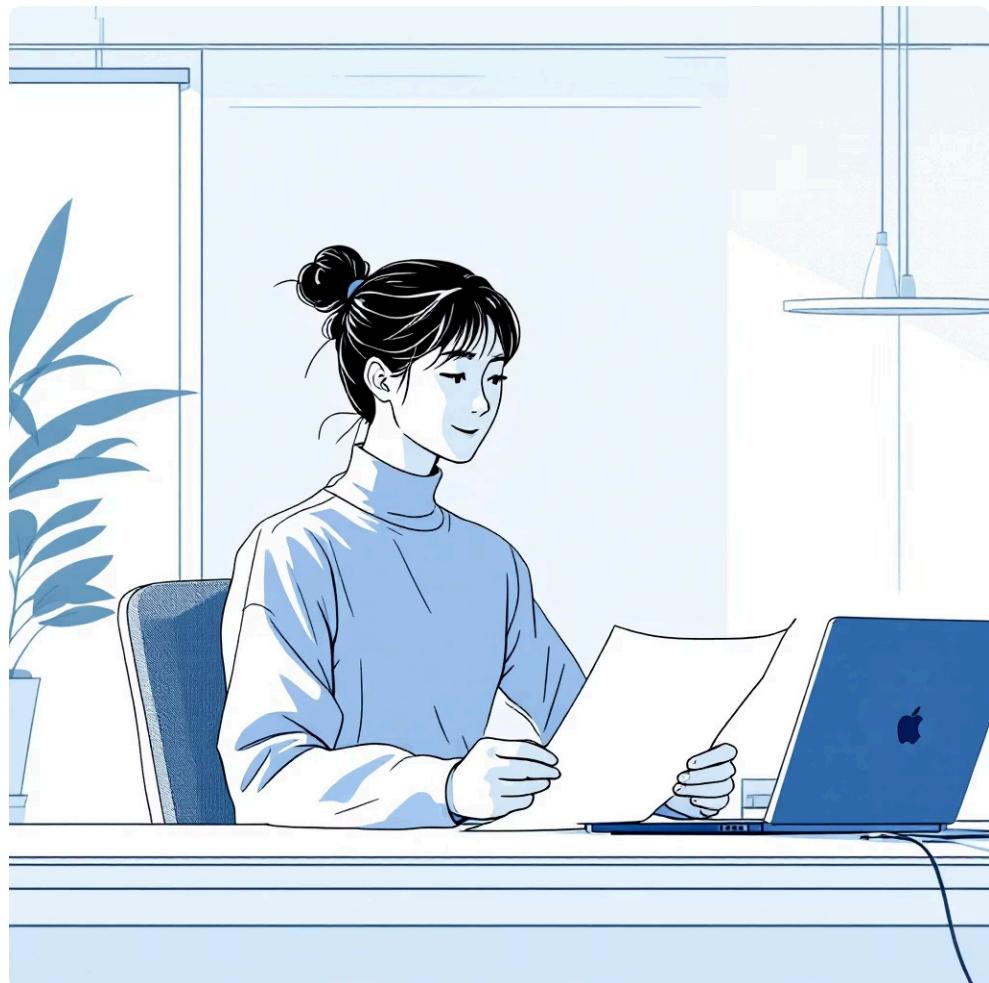
Exemplos de motivos válidos para negar:

- Essa informação contém dados pessoais de pacientes, protegidos pela LGPD
- Essa informação é sigilosa conforme Lei de Segurança Nacional
- Essa informação prejudicaria investigação em andamento

Importante: Nunca diga apenas 'não posso' ou 'não tenho'. Sempre justifique com base em lei.

Linguagem Cidadã: Escrevendo para Ser Entendido

Transparência não funciona se ninguém entender. Use linguagem simples e acessível.



✗ JARGÃO: 'Hipertensão arterial sistêmica'

✓ CLARO: 'Pressão alta'

✗ JARGÃO: 'Protocolo de triagem com escala de Manchester'

✓ CLARO: 'Ordem de atendimento por gravidade'

✗ JARGÃO: 'Medicação anti-hipertensiva de primeira linha'

✓ CLARO: 'Remédio para pressão alta'

✗ JARGÃO: 'Procedimento de anamnese estruturada'

✓ CLARO: 'Entrevista com o paciente para conhecer seu histórico'

Teste sua resposta: Leia em voz alta. Se você tropeçar nas palavras, o cidadão também vai tropeçar. Simplifique.

Dados Abertos: Conceito e Benefícios

Dados abertos são informações públicas disponibilizadas em formato que qualquer pessoa pode acessar, usar e compartilhar.



O que são dados abertos?

- Informações públicas em formato digital
- Sem restrições de acesso
- Em formato reutilizável (CSV, JSON, XML)
- Com licença aberta

Exemplos de dados abertos:

- Número de atendimentos por mês
- Medicamentos em falta
- Horários de funcionamento
- Protocolos de atendimento
- Estatísticas de saúde

Benefícios:

- Cidadão pode analisar dados
- Pesquisadores podem fazer estudos
- Jornalistas podem investigar
- Reduz pedidos de LAI
- Aumenta confiança na instituição

Onde publicar?

- Portal da Transparência
- Site da instituição
- Plataformas de dados abertos (dados.gov.br)

Portal da Transparência: O Que Publicar e Como

O Portal da Transparência é o lugar onde você publica informações para que o cidadão as encontre facilmente.

01

Identifique informações públicas

Orçamento, licitações, salários, protocolos, estatísticas

02

Organize em categorias

Saúde, Finanças, Recursos Humanos, Atendimento

03

Publique em formato acessível

PDF, Excel, CSV (não apenas imagens)

04

Atualize regularmente

Dados desatualizados são piores que nenhum dado

05

Facilite a busca

Use títulos claros, descrições, datas de atualização

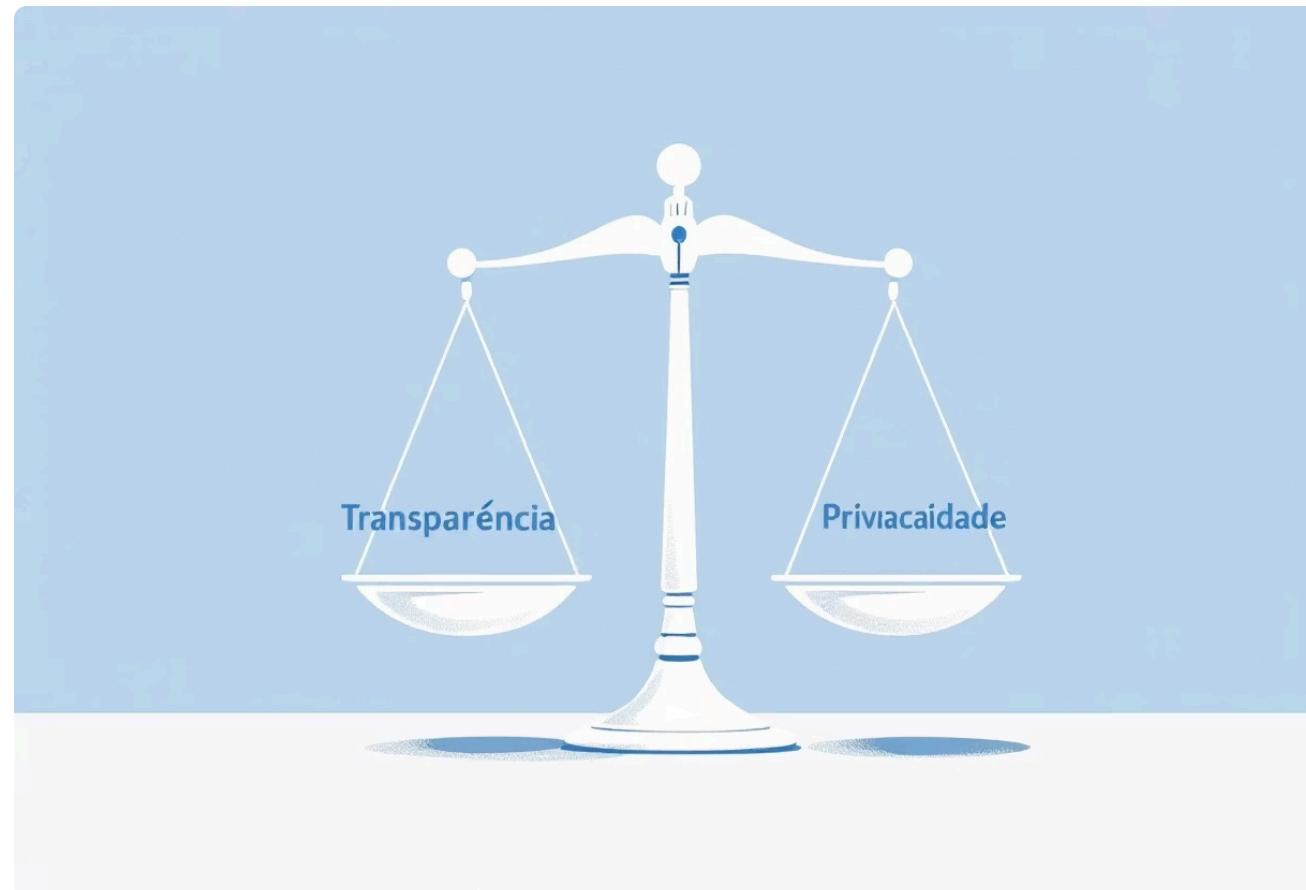
Checklist para publicação:

- Informação é pública? (não contém dados pessoais)
- Está em linguagem clara?
- Está em formato reutilizável?
- Tem data de atualização?
- Tem descrição clara?
- Está organizada logicamente?

Transparência ativa bem feita reduz 80% dos pedidos de LAI. Vale o investimento!

Integração LGPD + LAI: Balanceando Transparéncia e Proteção

Às vezes, você enfrenta um dilema: a informação é pública (LAI) mas contém dados pessoais (LGPD). Como resolver?



Regra de Ouro: LGPD SEMPRE PREVALECE

Quando há conflito entre LAI e LGPD, a proteção de dados pessoais vem em primeiro lugar.

Exemplos de decisão:

Estratégia: Anonimizar dados

- Remova nomes, CPF, datas de nascimento
- Mantenha informações estatísticas
- Exemplo: '347 pacientes' em vez de 'João Silva, Maria Santos, etc.'

Quando em dúvida: Consulte a supervisão e o setor jurídico.

Pergunta: 'Quem são os pacientes com diabetes?'

Resposta: Não posso compartilhar nomes (LGPD), mas posso dizer quantos pacientes têm diabetes (LAI)

Pergunta: 'Qual é o salário do Dr. João?'

Resposta: Não posso compartilhar (LGPD), mas posso dizer a faixa salarial de médicos em geral

Pergunta: 'Qual é o protocolo de atendimento?'

Resposta: Posso compartilhar (não contém dados pessoais)



Você Completou o Módulo 3!

LAI e Transparência Ativa

Parabéns! Você agora entende como garantir o direito à informação e comunicar com clareza com os cidadãos.

Lembre-se dos Princípios Fundamentais:

TRANSPARÊNCIA ATIVA

- Publique informações SEM ser pedido
- Use o Portal da Transparência
- Atualize regularmente
- Reduza pedidos de LAI

TRANSPARÊNCIA PASSIVA

- Responda em 20 dias
- Emita protocolo
- Justifique negativas
- Seja claro e completo

LINGUAGEM CIDADÃ

- Evite jargão técnico
- Explique termos complexos
- Organize bem a informação
- Teste a clareza

INTEGRAÇÃO LGPD + LAI

- LGPD sempre prevalece
- Anonimize dados pessoais
- Mantenha estatísticas
- Consulte quando em dúvida

Você está ajudando a construir um serviço público mais transparente, confiável e acessível para todos os cidadãos.

Nos vemos no próximo módulo!

MÓDULO 4: NOVAS TECNOLOGIAS E EFICIÊNCIA

Transformação Digital no Serviço Público

Descubra como ferramentas digitais podem melhorar sua produtividade e o atendimento aos cidadãos

O Que É Transformação Digital?

Transformação digital não é apenas usar computadores. É mudar a forma como trabalhamos, usando tecnologia para fazer as coisas melhor, mais rápido e com menos erros.



01

Antes: Papéis, filas, demora, erros manuais

02

Agora: Sistemas digitais, agendamento online, dados automáticos

03

Resultado: Menos tempo, mais eficiência, melhor atendimento

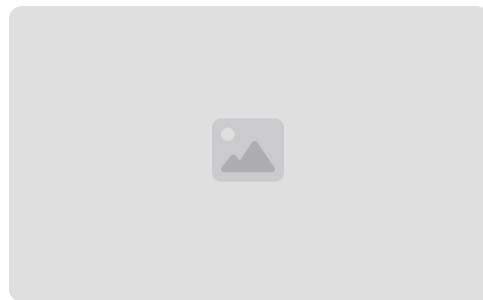
04

Benefício: Você trabalha menos com burocracia, mais com pessoas

- Transformação digital é para TODOS, não apenas para quem é 'tech'. Você aprende no seu ritmo.

Ferramentas de Produtividade: Office 365 e Google Workspace

Essas ferramentas permitem que você trabalhe de forma colaborativa, compartilhando documentos e editando em tempo real com seus colegas.



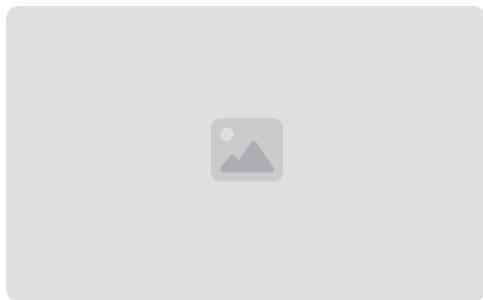
Word/Google Docs: Criar e editar documentos juntos

Vários colegas podem editar o mesmo documento ao tempo, sem perder informações



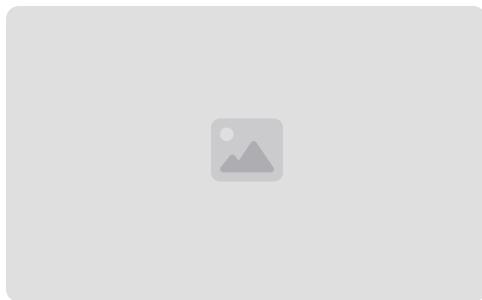
Excel/Google Sheets: Planilhas colaborativas

Organize dados, crie gráficos e compartilhe com a equipe em tempo real



PowerPoint/Google Slides: Apresentações

Crie apresentações profissionais e compartilhe com facilidade



OneDrive/Google Drive: Armazenamento em nuvem

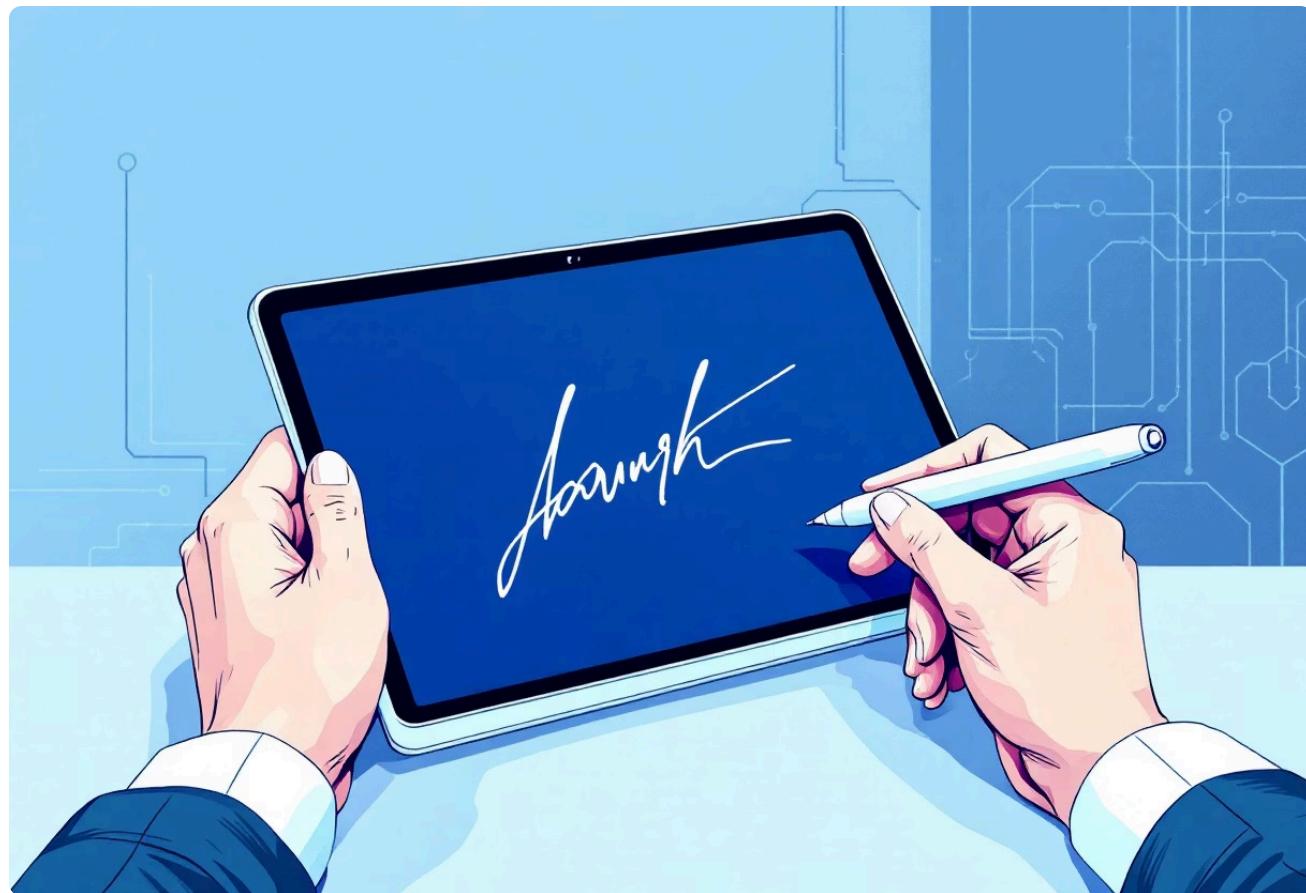
Acesse seus arquivos de qualquer lugar, em qualquer dispositivo

- Dica: Use a nuvem institucional, não a pessoal, para guardar dados de trabalho!

Assinatura Digital e Reuniões Virtuais

Duas ferramentas que transformam como você trabalha: assinatura digital elimina papéis, reuniões virtuais eliminam deslocamentos.

Assinatura Digital



A assinatura digital é tão válida quanto a manuscrita. Você pode assinar documentos sem imprimir, economizando tempo e papel.

Boas práticas:

Use plataformas oficiais (ICP-Brasil)

Guarde sua senha com segurança

Verifique o documento antes de assinar

Teste áudio e vídeo antes

Escolha local silencioso

Desligue notificações

Seja pontual

Reuniões Virtuais



Reúna-se com colegas sem sair do seu lugar. Economize tempo de deslocamento e seja mais produtivo.

Boas práticas:

Inteligência Artificial Desmistificada

IA não é ficção científica. É uma ferramenta que aprende com dados para ajudar você a trabalhar melhor.



O que IA **NÃO** é:

- **✗** Não é um robô que vai roubar seu emprego
- **✗** Não é mágica ou sobrenatural
- **✗** Não é perfeita

O que IA **É**:

- **✓** Uma ferramenta que reconhece padrões
- **✓** Que aprende com exemplos
- **✓** Que pode ajudar você a ser mais produtivo

Exemplos práticos:



Chatbots que respondem perguntas comuns



Tradutores automáticos



Organizadores de tarefas



Sugestões de correção de texto

Cuidados Éticos: Limites da IA

IA é poderosa, mas tem limites. Você precisa saber quando usá-la e quando não usar.

⚠ Dados Sensíveis: Nunca compartilhe dados de pacientes com ferramentas de IA públicas

Use apenas ferramentas aprovadas pela instituição

⚠ Verificação: IA pode cometer erros. Sempre verifique as respostas

Não confie cegamente em sugestões de IA

⚠ Decisões Críticas: IA não deve tomar decisões sobre saúde sozinha

Sempre há um profissional responsável pela decisão final

⚠ Transparência: Informe quando está usando IA

O cidadão tem direito de saber se está falando com um chatbot ou uma pessoa

IA é uma ferramenta para AJUDAR você, não para SUBSTITUIR seu julgamento profissional.

Atendimento Digital ao Cidadão

O cidadão quer ser atendido de forma rápida e fácil. Canais digitais permitem isso.



Agendamento Online

Cidadão marca consulta sem sair de casa, 24 horas por dia

Chatbot de Atendimento

Responde perguntas comuns automaticamente, liberando você para casos complexos

Atendimento por E-mail

Responda dúvidas de forma documentada e rastreável

Acessibilidade Digital

Seu site/sistema deve funcionar para pessoas com deficiência visual, auditiva, motora

- ☐ Acessibilidade não é um luxo, é um direito. Todos devem conseguir usar o serviço público.

Medindo Eficiência: Métricas Simples

Como saber se a transformação digital está funcionando? Meça o que importa.

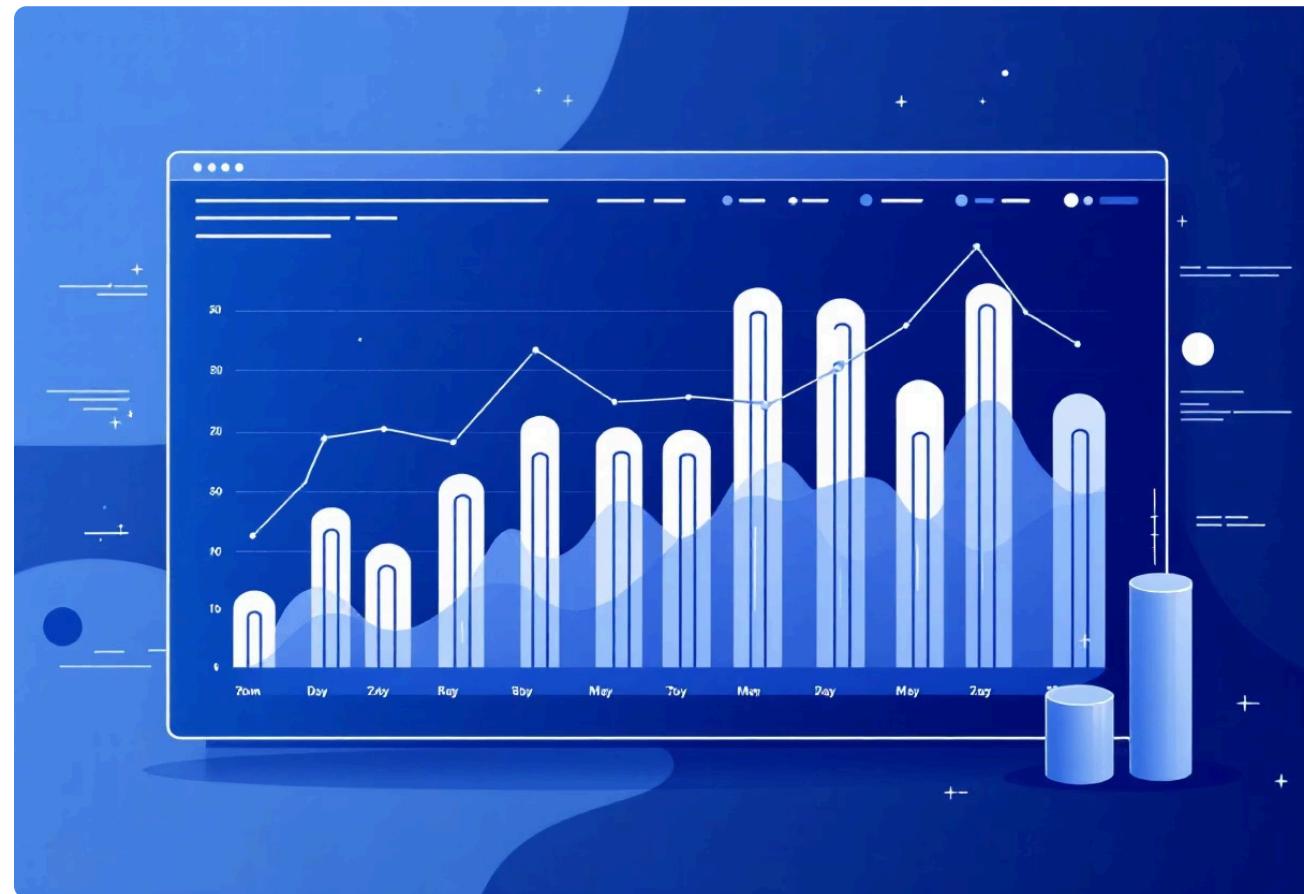
Métricas simples que você pode acompanhar:

01

Tempo de Atendimento

Antes: 30 minutos por paciente

Depois: 15 minutos (com agendamento online)



02

Erros Reduzidos

Antes: Dados digitados manualmente

Depois: Dados automáticos = menos erros

03

Satisfação do Cidadão

Pergunta simples: 'Você ficou satisfeito?'

Acompanhe as respostas ao longo do tempo

04

Produtividade da Equipe

Quantas tarefas você consegue fazer por dia?

Acompanhe a evolução

Lembre-se: Não é sobre fazer mais, é sobre fazer MELHOR.

Principais Aprendizados do Módulo 4



Transformação Digital: Mudar como trabalhamos, não apenas usar computadores



Colaboração: Trabalhe junto com colegas em tempo real



IA é Ferramenta: Ajuda você, não substitui seu julgamento



Segurança Sempre: Dados sensíveis em ferramentas aprovadas



Acessibilidade: Todos devem conseguir usar o serviço



Meça Resultados: Acompanhe tempo, erros, satisfação

Você Completou o Módulo 4!

Novas Tecnologias e Eficiência

Parabéns! Você agora entende como a tecnologia pode transformar seu trabalho e melhorar o atendimento aos cidadãos.

Lembre-se:

- Transformação digital é para todos
- Ferramentas colaborativas aumentam produtividade
- IA é uma aliada, não uma ameaça
- Segurança sempre vem em primeiro lugar
- Acessibilidade é direito, não luxo
- Meça resultados para melhorar continuamente
- Quando em dúvida, peça ajuda ao TI

Você está ajudando a construir um serviço público mais moderno, eficiente e acessível para todos.

Parabéns por completar este curso de capacitação digital! Você agora tem as ferramentas e conhecimento para trabalhar com segurança, privacidade e eficiência no serviço público de saúde.

